Detech it easy phát hiện packer VMProtect.

Load vào x64dgb.

Tìm module VirtualProtect trong kernel32.dll và set breakpoint tại cuối VirtualProtect

Graphical user interface, application, Word

Description automatically generated

Đặt breakpoint ở cuối

Text

Description automatically generated

.text segment trước khi call virtual protect sẽ không chứa dữ liệu, nhưng sau khi call virtual protect sẽ có chứa code. Ta debug cho tới khi breakpoint tại VirtualProtect hit. Sau đó xem code trong .text

Sau một vài lần F9 thì đây là code trong .text

Text

Description automatically generated

Check trong stack view: Follow stack view

Graphical user interface, text, application

Description automatically generatedĐi theo chiều tăng của stack, nếu thấy return to kernel32 đầu tiên thì đặt hardware breakpoint on access vào đó (đặt breakpoint ở dòng trước dòng đó) (tips: dòng màu đỏ)

A picture containing text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Quay lại xóa breakpoint ở cuối VirtualProtect, F9 1 lần để chương trình dừng lại.  
Mở memory map, set breakpoint on access tại .text

Graphical user interface, application

Description automatically generated

Disable hardware breakpoint ở trên đi. F9 cho tới bao giờ tổ tiên mách bảo đó là EOP thì dừng lại. Kết quả: EOP: 0x41308

Text

Description automatically generated

Scylla dump ra, file vẫn chưa chạy được vì thiếu dll, nhưng analyze bằng IDA thấy detect được winmain chứng tỏ đã tìm đúng EOP.